

# Subset sums in abelian groups

Eric Balandraud <sup>\*</sup>      Benjamin Girard <sup>†</sup>      Simon Griffiths <sup>‡</sup>  
 Yahya ould Hamidoune

*To Yahya ould Hamidoune, an inspiration and a dear friend.*

## Abstract

Denoting by  $\Sigma(S)$  the set of subset sums of a subset  $S$  of a finite abelian group  $G$ , we prove that

$$|\Sigma(S)| \geq \frac{|S|(|S|+2)}{4} - 1$$

whenever  $S$  is symmetric,  $|G|$  is odd and  $\Sigma(S)$  is aperiodic. Up to an additive constant of 2 this result is best possible, and we obtain the stronger (exact best possible) bound in almost all cases. We prove similar results in the case  $|G|$  is even. Our proof requires us to extend a theorem of Olson on the number of subset sums of anti-symmetric subsets  $S$  from the case of  $\mathbb{Z}_p$  to the case of a general finite abelian group. To do so, we adapt Olson's method using a generalisation of Vosper's Theorem proved by Hamidoune and Plagne.

## 1 Introduction

The study of the set of subset sums

$$\Sigma(S) = \left\{ \sum_{x \in X} x : X \subseteq S \right\} \tag{1}$$

of a subset  $S$  of a finite abelian group  $G$  is well established within the field of Additive Number Theory and was a recurring theme in the research of Yahya ould Hamidoune through the years. His contributions here, and on the related problem of the restricted sumset, have greatly increased our understanding.

The study of subset sums may be traced back to the 1964 paper of Erdős and Heilbronn [4]. They consider the question of determining the minimum  $\ell \in \mathbb{N}$  such that every subset  $S \subseteq \mathbb{Z}_p \setminus \{0\}$  ( $p$  prime) with  $|S| \geq \ell$  covers  $\mathbb{Z}_p$  with its subset sums, i.e., satisfies  $\Sigma(S) = \mathbb{Z}_p$ . They proved that  $\Sigma(S) = \mathbb{Z}_p$  provided  $|S| \geq 3\sqrt{6}\sqrt{p}$ .

---

<sup>\*</sup>IMJ, Équipe Combinatoire et Optimisation, Université Pierre et Marie Curie (Paris 6), 4 place Jussieu, 75005 Paris, France, email: [balandraud@math.jussieu.fr](mailto:balandraud@math.jussieu.fr).

<sup>†</sup>IMJ, Équipe Combinatoire et Optimisation, Université Pierre et Marie Curie (Paris 6), 4 place Jussieu, 75005 Paris, France, email: [bgirard@math.jussieu.fr](mailto:bgirard@math.jussieu.fr).

<sup>‡</sup>IMPA, Estrada Dona Castorina 110, Rio de Janeiro, Brasil, 22460-320, email: [sgriff@impa.br](mailto:sgriff@impa.br). Research supported by CNPq Proc. 500016/2010-2.

The same question may be considered in an arbitrary finite abelian group. In fact, in this case the *critical number* of a finite abelian group  $G$ ,

$$\text{cr}(G) = \min\{\ell : \Sigma^*(S) = G \text{ for all } S \subseteq G \setminus \{0\}, |S| \geq \ell\},$$

is defined in terms of  $\Sigma^*(S)$ , the set of all non-empty subset sums of  $S$ , but this difference is not of any great importance to the present discussion. Improving on the result of Erdős and Heilbronn [4], Olson [14] proved that  $\text{cr}(\mathbb{Z}_p) \leq 2\sqrt{p}$ . The precise result that  $\text{cr}(\mathbb{Z}_p) = \lfloor 2(\sqrt{p-2}) \rfloor$  for all primes  $p \geq 3$  follows from Theorem 4.2 and Example 4.2 of Dias da Silva and Hamidoune [3] (using the observation that  $4p-7$  is not a square for any prime  $p \geq 3$ ). The critical number is now known precisely for every finite abelian group, see the article of Freeze, Gao and Geroldinger [5] and the references contained therein.

A closely related problem to the determination of  $\text{cr}(G)$  is the problem of proving bounds on  $|\Sigma(S)|$ . Indeed, Erdős and Heilbronn [4] proved their bound on  $\text{cr}(\mathbb{Z}_p)$  by proving a quadratic lower bound on  $|\Sigma(S)|$  for subsets  $S \subseteq \mathbb{Z}_p$  and Olson [14] improved on their result by proving the following lower bound on  $|\Sigma(S)|$ . We remark that the bound is best possible in almost all cases, the exceptional case being the case when  $|\Sigma(S)|$  is almost as large as  $|G|/2$  in which case  $\xi(S) = 0$ . For a subset  $S$  of a finite abelian group  $G$ , we denote by  $\langle S \rangle$  the subgroup generated by  $S$ , and the parameter  $\xi(S)$  is defined to be identically 1 if  $|S|$  is even and as follows in the case  $|S|$  is odd:

$$\xi(S) = \begin{cases} 1 & \text{if } 2|S|^2 + 3|S| \leq 2|\langle S \rangle| + 5 \\ 0 & \text{if } 2|S|^2 + 3|S| > 2|\langle S \rangle| + 5. \end{cases}$$

**Theorem 1.1** (Olson). *Let  $G = \mathbb{Z}_p$  where  $p$  is prime, and let  $S$  be a subset of  $G$  such that  $S \cap (-S) = \emptyset$ . Then one of the following holds.*

(i)

$$|\Sigma(S)| \geq \frac{|S|(|S|+1)}{2} + \xi(S).$$

(ii)

$$|\Sigma(S)| > \frac{p}{2}.$$

In the case of a general finite abelian group, non-trivial subgroups present an obstacle to extending Olson's Theorem. For this reason we consider the following to be the natural extension of Olson's Theorem to the case of a general finite abelian group.

**Theorem 1.2.** *Let  $G$  be a finite abelian group, and let  $S \subseteq G$  be such that  $S \cap (-S) = \emptyset$  and  $|S| \geq 2$ . Then one of the following holds.*

(i)

$$|\Sigma(S)| \geq \frac{|S|(|S|-1)}{2} + 3.$$

(ii) *There is a non-empty subset  $S' \subseteq S$  for which*

$$|\Sigma(S')| > \frac{|\langle S' \rangle|}{2}.$$

Furthermore, if  $|G|$  is odd then property (i) may be replaced by

(i')

$$|\Sigma(S)| \geq \frac{|S|(|S|+1)}{2} + \xi(S).$$

We now describe a consequence of Theorem 1.2 (see Theorem 1.5 below) that was in fact our main motivation for proving it.

The fact that  $|\Sigma(S)|$  exhibits quadratic growth as a function of  $|S|$  was established by Erdős and Heilbronn for subsets  $S \subseteq \mathbb{Z}_p$ . The analogous result for general finite abelian groups was established by DeVos, Goddyn, Mohar and Šámal [2]. We say that a subset  $X$  of a finite abelian group  $G$  is *aperiodic* if the equality  $X + g = X$  is satisfied only for  $g = 0$ .

**Theorem 1.3** (DeVos, Goddyn, Mohar and Šámal). *Let  $G$  be a finite abelian group, and  $S \subseteq G \setminus \{0\}$  a subset for which  $\Sigma(S)$  is aperiodic. Then  $|\Sigma(S)| \geq |S|^2/64$ .*

It is believed that  $\frac{1}{64}$  may be replaced by  $\frac{1}{4}$ . The natural extremal example that shows that  $\frac{1}{4}$  would be best possible is the subset  $S = \{\pm 1, \dots, \pm s\} \subseteq \mathbb{Z}_n$ , where  $n > s(s+1)+1$ . This set  $S$  has  $|S| = 2s$  and  $|\Sigma(S)| = s(s+1)+1 = s^2 + s + 1$ . We note that the set  $S$  is symmetric (i.e.,  $S = -S$ ) and remark that we believe in general that such extremal examples should be symmetric (or very close to symmetric). This belief is supported by the fact [7], that we may replace the fraction  $\frac{1}{64}$  of Theorem 1.3 by  $\frac{1}{4} - o(1)$  in general and by  $\frac{1}{2} - o(1)$  in the case that  $S \cap (-S) = \emptyset$ . Indeed, by adapting the approach of [7] slightly one obtains that  $\frac{1}{64}$  may be replaced by  $\frac{1}{4}$  provided that  $S$  is large and far from being symmetric.

**Theorem 1.4.** *For all  $\epsilon > 0$  there exists a constant  $n_0 = n_0(\epsilon)$  such that the following holds. Let  $G$  be a finite abelian group, and  $S \subseteq G \setminus \{0\}$  a subset with  $|S \Delta (-S)| \geq \epsilon|S|$ ,  $|S| \geq n_0$  and for which  $\Sigma(S)$  is aperiodic. Then  $|\Sigma(S)| \geq (\frac{1}{4} + \epsilon^2)|S|^2$ .*

We hope it is now clear to the reader that symmetric sets  $S \subseteq G$  are of particular interest. We may deduce from Theorem 1.2 the following bounds on the number of subset sums of symmetric sets. For a symmetric set  $S$  we write  $\xi'(S)$  for  $\xi(S')$  where  $S'$  is any subset of  $S$  with  $|S'| = |S|/2$  and  $S = S' \cup (-S')$ . Equivalently

$$\xi'(S) = \begin{cases} 1 & \text{if } \frac{1}{2}|S|^2 + \frac{3}{2}|S| \leq 2|\langle S \rangle| + 5 \\ 0 & \text{if } \frac{1}{2}|S|^2 + \frac{3}{2}|S| > 2|\langle S \rangle| + 5. \end{cases}$$

**Theorem 1.5.** *Let  $G$  be a finite abelian group, and  $S \subseteq G \setminus \{0\}$  a symmetric subset with  $|S| \geq 4$  for which  $\Sigma(S)$  is aperiodic. Then*

$$|\Sigma(S)| \geq \frac{|S|(|S|-2)}{4} + 5.$$

Furthermore, if  $|G|$  is odd then

$$|\Sigma(S)| \geq \frac{|S|(|S|+2)}{4} + 2\xi'(S) - 1.$$

By considering the example  $S = \{\pm 1, \dots, \pm s\} \subseteq \mathbb{Z}_n$  given above we observe that the latter bound is best possible (except in the exceptional case that  $\xi'(S) = 0$ ). We conjecture that this bound should hold even if the conditions that  $S$  is symmetric and  $|G|$  is odd are dropped.

**Conjecture 1.6.** *Let  $G$  be a finite abelian group, and  $S \subseteq G \setminus \{0\}$  a subset for which  $\Sigma(S)$  is aperiodic. Then*

$$|\Sigma(S)| \geq \frac{|S|(|S| + 2)}{4} + 1.$$

We remark also that similar results may be proved when  $\Sigma(S)$  has a non-trivial period (stabiliser). For a subset  $X \subseteq G$  we let

$$K = K(X) = \{g \in G : X + g = X\},$$

and refer to  $K$  as the *period* of  $X$ . In addition,  $X$  will be called *H-periodic* whenever  $H$  is a subgroup of  $G$  contained in  $K$ .

**Theorem 1.7.** *Let  $G$  be a finite abelian group,  $S \subseteq G$  a symmetric subset and  $K$  the period of  $\Sigma(S)$ . Then*

$$|\Sigma(S)| \geq \frac{|S \setminus K|(|S \setminus K| - 2)}{4} + |K|.$$

The outline of the article is as follows. In Section 2, we show how Theorems 1.5 and 1.7 may be deduced from Theorem 1.2. The only tools we shall require in Section 2 are Kneser's Addition Theorem and the so-called prehistoric lemma. In Section 3, we introduce the main tools and techniques that we shall require for the proof of Theorem 1.2. Curiously a technique introduced by Erdős and Heilbronn [4] and sharpened by Olson [14] remains at the heart of our proof. The proof of Theorem 1.2 appears in Section 4.

We remark that an extension of Olson's result in  $\mathbb{Z}_p$  has recently been obtained by one of the authors [1].

## 2 Subset sums of symmetric sets: Theorems 1.5 and 1.7

In this section, we deduce Theorems 1.5 and 1.7 from Theorem 1.2. We shall require Kneser's Addition Theorem, the prehistoric lemma and a simple observation concerning aperiodic sets. As usual for subsets  $X, Y \subseteq G$  we let  $X + Y := \{x + y : x \in X, y \in Y\}$ .

**Theorem 2.1** (Kneser's Addition Theorem, [11, 12, 13, 16]). *Let  $X, Y$  be two subsets of a finite abelian group  $G$ , and let  $H$  be the period of  $X + Y$ . Then*

$$|X + Y| \geq |X + H| + |Y + H| - |H|.$$

We include a second statement in the prehistoric lemma which is an immediate consequence of the first and will be useful in many of our applications of the lemma.

**Lemma 2.2** (Prehistoric Lemma). *If  $X, Y$  are two subsets of a finite abelian group  $G$  and  $|X| + |Y| > |G|$  then  $X + Y = G$ . Furthermore, if  $H \subseteq G$  is a subgroup,  $X \subseteq Q, Y \subseteq R$  are subsets of  $H$ -cosets  $Q$  and  $R$  and  $|X| + |Y| > |H|$  then  $X + Y = Q + R$ .*

**Observation 2.3.** *If  $\Sigma(S)$  is aperiodic and  $T \subseteq S$ , then  $\Sigma(T)$  is aperiodic. If  $\Sigma(S)$  has period  $K$  and  $T \subseteq S$ , then the set  $\{Q \in G/K : \Sigma(T) \cap Q \neq \emptyset\}$  is aperiodic in  $G/K$ .*

Let us now deduce Theorem 1.5 from Theorem 1.2.

*Proof of Theorem 1.5.* We prove the first bound, the second bound follows with an identical proof except using property (i') rather than (i) in the application of Theorem 1.2. Let  $G$  be a finite abelian group, and  $S \subseteq G \setminus \{0\}$  a symmetric subset with  $|S| \geq 4$  for which  $\Sigma(S)$  is aperiodic. If  $S$  contains an element  $x$  of order two then  $\Sigma(\{x\}) = \{0, x\}$  is not aperiodic, a contradiction, by the above observation. Thus we may assume that  $S$  contains no element of order two. It follows that  $S$  contains a subset  $S_+$  of cardinality  $|S_+| = |S|/2$  such that  $S = S_+ \cup (-S_+)$  and  $S_+ \cap (-S_+) = \emptyset$ .

By applying Theorem 1.2 to  $S_+$  we obtain that either  $|\Sigma(S_+)| \geq 3 + |S_+|(|S_+| - 1)/2$  or  $S_+$  contains a non-empty subset  $S'$  such that  $|\Sigma(S')| > |S'|/2$ . In the first case we note that, by symmetry, the same bound also applies to  $|\Sigma(-S_+)|$ , and so by an application of Kneser's Addition Theorem (and using the fact that  $\Sigma(S) = \Sigma(S_+) + \Sigma(-S_+)$  is aperiodic) we have that

$$|\Sigma(S)| \geq |\Sigma(S_+)| + |\Sigma(-S_+)| - 1 \geq 2 \left( \frac{(|S|/2)(|S|/2 - 1)}{2} + 3 \right) - 1 = \frac{|S|(|S| - 2)}{4} + 5,$$

as required. In the second case we note that, by symmetry,  $|\Sigma(-S')| > |S'|/2$ , and so  $\Sigma(S'), \Sigma(-S') \subseteq \langle S' \rangle$  are such that  $|\Sigma(S')| + |\Sigma(-S')| > |S'|$  and so

$$\Sigma(S' \cup (-S')) = \Sigma(S') + \Sigma(-S') = \langle S' \rangle$$

by the prehistoric lemma. However, this implies that  $\Sigma(S' \cup (-S'))$  is not aperiodic, a contradiction, by the above observation, and the proof is complete.  $\square$

We now prove Theorem 1.7.

*Proof of Theorem 1.7.* Since  $0 \in \Sigma(S)$ , we readily have  $\Sigma(S) \supseteq K$ , so that  $|\Sigma(S)| \geq |K|$ . This yields the desired result if  $S \setminus K = \emptyset$ . Thus, we can assume that  $S \setminus K \neq \emptyset$ . Now, note that it suffices to prove the inequality for  $T := S \setminus K$ . We associate to  $T$  a sequence of subsets of  $G/K$ . Let  $k := |K|$ . We define the sets  $T_1, \dots, T_k \subseteq G/K$  by

$$T_i := \{Q \in G/K : |T \cap Q| \geq i\} \quad i = 1, \dots, k,$$

and write  $l$  for the maximal  $i$  for which  $T_i$  is non-empty. Note that each of the sets  $T_i : i = 1, \dots, l$  is symmetric. The key observation is that an element of  $G$  belongs to  $\Sigma(T)$  if and only if the coset of  $K$  to which it belongs is an element of

$$\Sigma(T_1) + \dots + \Sigma(T_l).$$

So that

$$|\Sigma(T)| = k|\Sigma(T_1) + \dots + \Sigma(T_l)| \geq k(|\Sigma(T_1)| + \dots + |\Sigma(T_l)| - (l - 1)),$$

where the inequality follows from Kneser's Addition Theorem together with the observation that  $\Sigma(T_1) + \dots + \Sigma(T_l)$  is aperiodic in  $G/K$  (this follows from the definition of  $K$ ,

as an element of a  $K$ -coset that leaves  $\Sigma(T_1) + \dots + \Sigma(T_l)$  invariant under addition would also leave  $\Sigma(T)$  invariant under addition). Thus, to complete the proof of the theorem, it suffices to prove that

$$|\Sigma(T_1)| + \dots + |\Sigma(T_l)| \geq 2l + \frac{|T|(|T| - 2)}{4l}.$$

However, it follows immediately from the bound

$$|\Sigma(T_i)| \geq \frac{|T_i|(|T_i| - 2)}{4} + 2,$$

which is a consequence of Theorem 1.5 (which may be applied since  $T_i$  is symmetric and  $|\Sigma(T_i)|$  is aperiodic in  $G/K$ , see Observation 2.3), and the convexity of the function  $f(t) = t(t - 2)$ , that

$$|\Sigma(T_1)| + \dots + |\Sigma(T_l)| \geq 2l + \sum_{i=1}^l \frac{|T_i|(|T_i| - 2)}{4} \geq 2l + \frac{1}{l} \frac{|T|(|T| - 2)}{4},$$

which completes the proof.  $\square$

### 3 Some tools and techniques

In this section, we present the tools and techniques on which we base our proof of Theorem 1.2. Our approach is very similar in spirit to the approach of Olson [14]. His method, a refinement of that of Erdős and Heilbronn, is inductive. However, rather than considering only a single base case (such as  $|S| = 1$ ), he proves the required bound directly for all arithmetic progressions, and these become the base cases of the inductive proof. For the inductive step he may then assume that  $S$  is not an arithmetic progression in which case (with some work) one may find an element  $x \in S$  such that  $|\Sigma(S)| - |\Sigma(S \setminus \{x\})|$  is large, and the proof is completed by applying the induction hypothesis to  $S \setminus \{x\}$ .

In generalising Olson's approach we replace his dichotomy (whether or not  $S$  is an arithmetic progression) with the dichotomy of whether or not the set  $\hat{S} = S \cup \{0\} \cup (-S)$  is an arithmetic progression relative to a certain subgroup  $H$  of  $G$ , where  $H$ , a subgroup chosen as a function of  $\hat{S}$ , is given by applying the following theorem of Hamidoune and Plagne [10, Theorem 2.1] to  $\hat{S}$ . This result from critical pair theory, whose proof relies on the so-called *isoperimetric method*, may be seen as a generalisation of Vosper's Theorem to the general case of finite abelian groups. Before stating the result, we recall the following terminology. A subset  $X$  of a finite abelian group  $G$  is a *Vosper subset* in  $G$  if for any  $Y \subseteq G$ , with  $|Y| \geq 2$ , the inequality

$$|X + Y| \geq \min(|G| - 1, |X| + |Y|)$$

holds. Notice that a Vosper subset with cardinality one cannot exist in a group with cardinality four or more. In what follows, we denote by  $\phi$  the canonical homomorphism from  $G$  to  $G/H$ .

**Theorem 3.1** (Hamidoune-Plagne). *Let  $A$  be a generating subset of a finite abelian group  $G$  such that  $0 \in A$ . Suppose also*

$$|A| \leq \frac{|G|}{2}.$$

*Then, there exists a subgroup  $H$  of  $G$  with*

$$|A + H| < \min(|G|, |H| + |A|)$$

*such that  $\phi(A)$  is either an arithmetic progression or a Vosper subset in  $G/H$ .*

We will also use the following theorem, proved recently by some of the authors [6], concerning  $k \wedge A := \{a_1 + \dots + a_k : a_i \in A \text{ distinct}\}$ . We call a coset of an elementary 2-subgroup of  $G$  a 2-coset.

**Theorem 3.2.** *Let  $A$  be a finite subset of an abelian group  $G$ , and let  $1 \leq k \leq |A| - 1$ . Then*

$$|k \wedge A| \geq |A|,$$

*unless  $k \in \{2, |A| - 2\}$  and  $A$  is 2-coset, in which case  $|k \wedge A| = |A| - 1$ .*

In particular, if  $H$  is a subgroup of  $G$  and  $A$  a subset of an  $H$ -coset such that  $|H|/2 < |A| \leq |H|$  then

$$|k \wedge A| \geq \min(|H| - 1, |A|). \quad (2)$$

We complete the section by recalling some key results related to Olson's method.

### 3.1 Olson's method

Let  $B \subseteq G$  and  $x \in G$ . We write

$$\lambda_B(x) = |(B + x) \setminus B|.$$

An interesting feature of this number is that if  $S \subseteq G$  and  $B = \Sigma(S)$ , then for all  $x \in S$ ,

$$|\Sigma(S)| \geq |\Sigma(S \setminus \{x\})| + \lambda_B(x). \quad (3)$$

Some immediate properties of  $\lambda_B$  are given in the following lemma.

**Lemma 3.3** (Olson, [14, 15]). *Let  $B$  and  $C$  be non-empty subsets of a finite abelian group  $G$  such that  $0 \notin C$ . Then, for all  $x, y \in G$ , we have*

$$\lambda_B(x) = \lambda_{G \setminus B}(x). \quad (4)$$

$$\lambda_B(x) = \lambda_B(-x). \quad (5)$$

$$\lambda_B(x + y) \leq \lambda_B(x) + \lambda_B(y). \quad (6)$$

$$\sum_{x \in C} \lambda_B(x) \geq |B|(|C| - |B| + 1). \quad (7)$$

We will also use the following lemma, which states that one can always swap an element  $x \in S$  for  $-x$  without changing the number of subset sums. In addition, the resulting set of subset sums is aperiodic if and only if  $\Sigma(S)$  is so.

**Lemma 3.4** (Olson, [14, 15]). *Let  $S$  be a non-empty subset of  $G \setminus \{0\}$ . For any  $x \in S$ , one has  $|\Sigma((S \setminus \{x\}) \cup \{-x\})| = |\Sigma(S)|$ . Furthermore,  $\Sigma((S \setminus \{x\}) \cup \{-x\})$  is aperiodic if and only if  $\Sigma(S)$  is so.*

The main idea in Olson's method is to find conditions which guarantee the existence of an element  $x \in S$  such that  $\lambda_B(x)$  is large.

**Lemma 3.5** (Olson [15]). *Let  $G$  be a finite abelian group and let  $S$  be a generating subset of  $G$  such that  $0 \notin S$ . Let  $B$  be a subset of  $G$  such that  $|B| \leq |G|/2$ . Then there exists  $x \in S$  such that*

$$\lambda_B(x) \geq \min \left( \frac{|B| + 1}{2}, \frac{|S \cup (-S)| + 2}{4} \right).$$

*Proof.* This result follows, using (5), by applying Lemma 3.1 of [15] to  $S \cup (-S)$ .  $\square$

We will also use the following lemma, which is a consequence of the main result in [8].

**Lemma 3.6** (Hamidoune). *Let  $S$  be a subset of a finite abelian group  $G$  such that  $S \cap (-S) = \emptyset$ . Then*

$$|\Sigma(S)| \geq 2|S|.$$

*Proof.* The proof follows easily by induction on  $|S| \geq 1$ . It trivially holds when  $|S| = 1$ , so assume  $|S| \geq 2$  and set  $B = \Sigma(S)$ . If  $|B| \geq |G| - 1$ , then since  $|S| \leq (|G| - 1)/2$  we obtain  $|B| \geq 2|S|$ . Otherwise, we have  $2 \leq |B| \leq |G| - 2$ . Now, by Lemma 3.5 applied to  $B$  or  $G \setminus B$ , and using (4), there exists  $x \in S$  such that  $\lambda_B(x) \geq 2$ . By (3),  $|B| \geq |\Sigma(S \setminus \{x\})| + 2 \geq 2|S|$ .  $\square$

From these two results, we deduce the following useful lemma.

**Lemma 3.7.** *Let  $S$  be a subset of a finite abelian group  $G$  such that  $S \cap (-S) = \emptyset$ ,  $|\Sigma(S)| \leq |G|/2$  and  $|S| \geq 4$ . Then*

$$|\Sigma(S)| \geq 2|S| + 1.$$

*Proof.* Set  $B = \Sigma(S)$ . Since  $|S| \geq 4$ , we have  $|B| \geq |S| + 1 = 5$ . Now, by Lemma 3.5 applied to  $B$ , there exists  $x \in S$  such that

$$\lambda_B(x) \geq \min(3, 5/2).$$

Thus,  $\lambda_B(x) \geq 3$ . Now, using Lemma 3.6 and (3),  $|B| \geq |\Sigma(S \setminus \{x\})| + 3 \geq 2(|S| - 1) + 3 = 2|S| + 1$ .  $\square$

## 4 Proof of Theorem 1.2

Let  $G$  be a finite abelian group and  $S \subseteq G$  a subset such that  $S \cap (-S) = \emptyset$  and  $|S| \geq 2$ . Without loss of generality we may assume that  $S$  generates  $G$ , and we set  $\hat{S} = S \cup \{0\} \cup (-S)$ . Our proof is inductive. However, there is a certain class of sets for which an inductive proof is not appropriate. Informally, these cases correspond to sets  $S$  for which the structure of  $\hat{S}$  resembles an arithmetic progression. These cases are dealt with directly



(see Proposition 4.1). With these cases as a base the theorem may then be proved by induction on  $|S|$ .

Given a generating subset  $A$  of a finite abelian group  $G$  such that  $0 \in A$  and  $|A| \leq |G|/2$ , we may apply the Hamidoune-Plagne Theorem (Theorem 3.1) to  $A$  to obtain a subgroup  $H$  of  $G$  with the properties that  $|A+H| < \min(|G|, |H|+|A|)$  and  $\phi(A)$  is either an arithmetic progression or a Vosper subset in  $G/H$  (where  $\phi$  denotes the canonical homomorphism from  $G$  to  $G/H$ ). In the case that  $\phi(A)$  is an arithmetic progression we say that  $A$  has an *AP-representation*. In the case that  $\phi(A)$  is a Vosper set we say that  $A$  has a *Vosper-representation*.

We shall deduce Theorem 1.2 from the following proposition and lemmas.

**Proposition 4.1.** *Let  $G$  be a finite abelian group, and let  $S \subseteq G$  be a generating subset such that  $S \cap (-S) = \emptyset$  and  $|S| \geq 4$ . If  $\hat{S}$  has an AP-representation, then one of the following holds.*

(i)

$$|\Sigma(S)| \geq \frac{|S|(|S|+1)}{2} + 1.$$

(ii) *There is a non-empty subset  $S' \subseteq S$  for which*

$$|\Sigma(S')| > \frac{|S'|}{2}.$$

The following two lemmas make claims concerning  $\max_{x \in S} \lambda_B(x)$  for subsets  $S, B$  of a finite abelian group  $G$ . These bounds, applied with  $B = \Sigma(S)$ , are precisely what is required for our inductive proof of Theorem 1.2.

**Lemma 4.2.** *Let  $G$  be a finite abelian group, and let  $B, S$  be subsets of  $G$  with  $|B| = b \leq |G|/2$  and  $|S| = s \geq 3$ . Assume  $S$  generates  $G$ , that  $S \cap (-S) = \emptyset$  and that  $\hat{S}$  has a Vosper-representation. Then*

$$\max_{x \in S} \lambda_B(x) > s - \frac{s(s-3)}{b}.$$

*In particular, if  $2b \geq s(s-3)$ , then*

$$\max_{x \in S} \lambda_B(x) \geq s - 1.$$

**Lemma 4.3.** *Let  $G$  be a finite abelian group of odd order, and let  $B, S$  be subsets of  $G$  with  $|B| = b \leq |G|/2$  and  $|S| = s \geq 3$ . Assume  $S$  generates  $G$ , that  $S \cap (-S) = \emptyset$  and that  $\hat{S}$  has a Vosper-representation. Let also  $t$  be an integer,  $1 \leq t \leq |G| - 1$ , and set*

$$t = r(2s+2) + q, \text{ where } -1 \leq q \leq 2s.$$

*Then*

$$\max_{x \in S} \lambda_B(x) \geq \frac{4(s+1)b(t-b+1)}{t(t+2s+6) + q(2s-q-2)}.$$

We now observe that Theorem 1.2 is an immediate consequence of the above proposition and lemmas. In fact the first part of Theorem 1.2 may be deduced from Proposition 4.1 and Lemma 4.2, while Lemma 4.3 is required for the stronger bound in the case  $|G|$  is odd.

In the proof of Theorem 1.2, we will refer to  $S$  as a *valid subset* of  $G$  whenever

$$|\Sigma(S')| \leq \frac{|\langle S' \rangle|}{2}$$

for all non-empty subsets  $S' \subseteq S$ .

*Proof of Theorem 1.2.* Let  $S$  be a generating subset of  $G$  such that  $S \cap (-S) = \emptyset$  and  $|S| \geq 2$ . We begin by proving the first part of Theorem 1.2. Without loss of generality, we may also assume that  $S$  is a valid subset of  $G$ , else property (ii) holds and the proof is complete. Now, setting  $\hat{S} = S \cup \{0\} \cup (-S)$ , Lemma 3.7 yields

$$|\hat{S}| = 2|S| + 1 \leq |\Sigma(S)| \leq |G|/2.$$

Thus, it follows from Theorem 3.1 that  $\hat{S}$  has either an AP-representation or a Vosper-representation. We must prove that

$$|\Sigma(S)| \geq \frac{|S|(|S| - 1)}{2} + 3.$$

The base cases that  $|S| = 2, 3$  may be checked by hand, while the base case that  $\hat{S}$  has an AP-representation follows from Proposition 4.1. We now proceed to the induction step.

Assume  $|S| = s \geq 4$  and that  $\hat{S}$  has a Vosper-representation. Let  $B = \Sigma(S)$  and  $b = |B|$ . Since  $S$  is a valid subset of  $G$ , one has  $b \leq |G|/2$ . We prove the required bound  $b \geq 3 + s(s - 1)/2$  by considering  $b = |\Sigma(S)| \geq |\Sigma(S \setminus \{x\})| + \lambda_B(x)$  for an appropriately chosen  $x \in S$ . An initial lower bound on  $b$  may be obtained by selecting an arbitrary element  $x \in S$  and using that

$$b = |\Sigma(S)| \geq |\Sigma(S \setminus \{x\})| \geq 3 + \frac{(s - 2)(s - 1)}{2},$$

where the final inequality follows from the induction hypothesis. It follows that

$$2b \geq 6 + (s - 2)(s - 1) > s(s - 3).$$

Now, by Lemma 4.2 there is an element  $x \in S$  with  $\lambda_B(x) \geq s - 1$ . Thus

$$|\Sigma(S)| \geq |\Sigma(S \setminus \{x\})| + \lambda_B(x) \geq 3 + \frac{(s - 2)(s - 1)}{2} + (s - 1) = 3 + \frac{s(s - 1)}{2},$$

as required.

For the second part of Theorem 1.2, the stronger bound in the case that  $|G|$  is odd, we proceed by induction with the same base cases. For the induction step, assume  $|S| = s \geq 4$  and that  $\hat{S}$  has a Vosper-representation. One can distinguish the following two cases.

**Case I.** There is an element  $x \in S$  such that  $\langle S \setminus \{x\} \rangle$  is a proper subgroup of  $\langle S \rangle$ .

In this case, the induction step is easy. We simply use that  $\xi(S \setminus \{x\}) \geq 0$  to obtain

$$|\Sigma(S)| = 2|\Sigma(S \setminus \{x\})| \geq (s-1)s \geq \frac{s(s+1)}{2} + 1.$$

**Case II.**  $\langle S \setminus \{x\} \rangle = \langle S \rangle$  for all  $x \in S$ .

Let  $B = \Sigma(S)$  and  $b = |B|$ . Since  $S$  is a valid subset of  $G$ , one has  $b \leq |G|/2$ . Arguing as in the first part of the proof, there exists an element  $x \in S$  such that  $\lambda_B(x) \geq s-1$ . It follows, by the induction hypothesis, that

$$\begin{aligned} |\Sigma(S)| &\geq |\Sigma(S \setminus \{x\})| + (s-1) \\ &\geq \frac{s(s-1)}{2} + \xi(S \setminus \{x\}) + s-1 \\ &= \frac{s(s+1)}{2} + \xi(S \setminus \{x\}) - 1. \end{aligned}$$

In the special case that  $\xi(S \setminus \{x\}) = 1$  and  $\xi(S) = 0$  this bound is sufficient to complete the proof. If  $\xi(S \setminus \{x\}) = 0$ , it follows that

$$2s^2 - s - 1 = 2(s-1)^2 + 3(s-1) > 2|\langle S \setminus \{x\} \rangle| + 5 = 2|\langle S \rangle| + 5,$$

and so

$$|\Sigma(S)| \geq \frac{s(s+1)}{2} - 1 = \frac{2s^2 + 2s - 4}{4} > \frac{2|\langle S \rangle|}{4} = \frac{|G|}{2},$$

a contradiction, since  $S$  is a valid subset of  $G$ . Thus, the only remaining case is that  $\xi(S \setminus \{x\}) = \xi(S) = 1$ . In particular we can assume that

$$\begin{cases} s^2 + s - 2 \leq |G| - 1 & \text{if } s \text{ is even} \\ s^2 + \frac{3}{2}s - \frac{7}{2} \leq |G| - 1 & \text{if } s \text{ is odd} \end{cases}$$

Since we have that  $b \geq s(s+1)/2$  and the proof is completed when we prove  $b \geq 1 + s(s+1)/2$  we may assume for contradiction that  $b = s(s+1)/2$ . However, one may now apply Lemma 4.3, with

$$t = \begin{cases} s^2 + s - 2 & \text{if } s \text{ is even} \\ s^2 + \frac{3}{2}s - \frac{7}{2} & \text{if } s \text{ is odd} \end{cases}$$

and

$$q = \begin{cases} 2s & \text{if } s \text{ is even} \\ \frac{3}{2}s - \frac{5}{2} & \text{if } s \text{ is odd} \end{cases}$$

to obtain that  $\max_{x \in S} \lambda_B(x) > s-1$ . In particular, there exists  $x \in S$  with  $\lambda_B(x) \geq s$  and so

$$|\Sigma(S)| \geq |\Sigma(S \setminus \{x\})| + s \geq \frac{s(s-1)}{2} + 1 + s = \frac{s(s+1)}{2} + 1,$$

as required.  $\square$

We prove Proposition 4.1 in Section 4.1 and Lemmas 4.2 and 4.3 in Sections 4.2 and 4.3 respectively.

#### 4.1 The case that $\hat{S}$ has an AP-representation: A proof of Proposition 4.1

Let  $G$  be a finite abelian group and  $S \subseteq G$  a generating subset such that  $S \cap (-S) = \emptyset$ ,  $|S| \geq 4$  and  $\hat{S}$  has an AP-representation. Let  $H$  be a subgroup of  $G$  with

$$|\hat{S} + H| < \min(|G|, |\hat{S}| + |H|) \quad (8)$$

and with  $\phi(\hat{S})$  being an arithmetic progression in  $G/H$ . We may also assume throughout the proof that

$$|\Sigma(S')| \leq \frac{|\langle S' \rangle|}{2} \quad (9)$$

for all non-empty subsets  $S' \subseteq S$  (i.e.,  $S$  is a valid subset of  $G$ ), else property (ii) of Proposition 4.1 holds and the proof is complete.

Now, since  $S$  is a generating subset of  $G$ , it follows that  $G/H$  is a cyclic group. Thus, we may write  $G/H$ , the group of  $H$ -cosets in  $G$ , as follows

$$G/H \simeq \mathbb{Z}/m\mathbb{Z} \simeq \{Q_i : i = 0, \dots, m-1\},$$

and we may assume, without loss of generality, that  $\phi(\hat{S})$  has difference  $Q_1$ , so that  $\phi(\hat{S}) = \{Q_{-v}, \dots, Q_v\}$ , for some  $v \geq 1$ . We consider the partition

$$\hat{S} = \hat{S}_{-v} \cup \dots \cup \hat{S}_{-1} \cup \hat{S}_0 \cup \hat{S}_1 \cup \dots \cup \hat{S}_v,$$

where  $\hat{S}_i = \hat{S} \cap Q_i$  for all  $i \in \{-v, \dots, v\}$ . Note that, by the symmetry of  $\hat{S}$ , we have  $\hat{S}_{-i} = -\hat{S}_i$  for all  $i \in \{-v, \dots, v\}$ . Since Lemma 3.4 allows us to swap an element  $x \in S$  for  $-x$  we may suppose that

$$S = S_0 \cup S_1 \cup \dots \cup S_v,$$

where  $S_i = \hat{S}_i$  for all  $i \in \{1, \dots, v\}$  and  $|\hat{S}_0| = 2|S_0| + 1$ .

We use the following notation:

$$t := |S_0| \quad u := \sum_{i=1}^v |Q_i \setminus S_i| \quad \text{and} \quad \ell := \sum_{i=1}^v i|S_i|,$$

and write  $h$  for  $|H|$ . Note that, in this notation,

$$|S| = vh + t - u,$$

and, by Lemma 3.6,

$$|\Sigma(S_0)| \geq 2t.$$

We now establish the following claims.

**Claim I.**  $t \leq h/4$ .

*Proof.* If  $|S_0| = t > h/4$ , then  $|\Sigma(S_0)| \geq 2t > h/2 \geq |\langle S_0 \rangle|/2$ , contradicting (9).  $\square$

**Claim II.**  $u \leq t$ .

*Proof.* Since  $|\hat{S}| = 2|S| + 1 = 2vh + 2t - 2u + 1$ , and  $|\hat{S} + H| = (2v + 1)h$ , it follows from (8) that

$$2t - 2u + 1 > 0,$$

and the required bound follows.  $\square$

**Claim III.**  $\ell \geq hv(v + 1)/2 - uv$ .

*Proof.* Since the cardinalities  $|S_1|, \dots, |S_v|$  obey  $0 \leq |S_i| \leq h$  and  $\sum_{i=1}^v |S_i| = vh - u$ , the sum  $\ell = \sum_{i=1}^v i|S_i|$  is minimised by taking  $|S_i| = h$  for  $i = 1, \dots, v - 1$  and  $|S_v| = h - u$ , and in this case one obtains  $\ell = hv(v + 1)/2 - uv$ .  $\square$

We now prove the key lemma from which we shall deduce our bound on  $|\Sigma(S)|$ . The idea behind the proof is that  $\Sigma(S)$  should contain all of the elements of all of the cosets  $Q_1, \dots, Q_{\ell-1}$  together with a few more elements in the case  $t > 0$ .

**Lemma 4.4.** *Let  $S, h, \ell, v$  and  $t$  be as defined above. Then  $|\Sigma(S)| \geq (\ell - 1)h + 4t$ .*

*Proof.* We prove the lemma under the assumption  $\ell < |G/H|$ , in which case the cosets  $Q_0, \dots, Q_\ell$  are disjoint. Since it may be easily verified (by a similar approach) that  $|\Sigma(S)| > |G|/2$ , contradicting (9), in the case that  $\ell \geq |G/H|$  we may safely restrict to this case.

We consider first the special case that  $v = 1$  and  $t = 0$ . It suffices to prove that  $\Sigma(S) \supseteq Q_j$  for  $j \in \{1, \dots, h - 1\} \setminus \{2, h - 2\}$ ,  $|\Sigma(S) \cap Q_j| \geq h - 1$  for  $j \in \{2, h - 2\}$  and  $|\Sigma(S) \cap Q_j| = 1$  for  $j \in \{0, \ell\} = \{0, h\}$ . To prove these bounds we note that  $\Sigma(S) \cap Q_j \supseteq j \wedge S$ , and the various claimed bounds are either trivial or follow from Theorem 3.2.

For the remaining cases we claim that

$$\Sigma(S) \supseteq \bigcup_{j=1}^{\ell-1} Q_j$$

and  $|\Sigma(S) \cap Q_j| \geq 2t$  for  $j \in \{0, \ell\}$ . It is immediate, since  $|\Sigma(S_0)| \geq 2t$ , that  $|\Sigma(S) \cap Q_j| \geq 2t$  for  $j \in \{0, \ell\}$ . The proof that  $\Sigma(S) \supseteq Q_j$  for all  $j \in \{1, \dots, \ell - 1\}$  proceeds slightly differently in the cases  $t = 0$  and  $t > 0$ . We note that this fact is trivial if  $h = 1$ , so we may assume that  $h \geq 2$ .

If  $t > 0$  then we recall that  $|\Sigma(S_0)| \geq 2t$  and that  $u \leq t$  (Claim II). We also have that  $h \geq 4$  (Claim I) and  $|S_i| \geq \frac{3}{4}h > 2$  for all  $i$  (Claims I and II). Fix  $j \in \{1, \dots, \ell - 1\}$  and note that, by the definition of  $\ell$ , there exists a sequence  $k_1, \dots, k_v$  such that

$$\sum_{i=1}^v ik_i = j$$

where  $0 \leq k_i \leq |S_i|$  for all  $i$ , and  $0 < k_{i_0} < |S_{i_0}|$  for some  $i_0 \in \{1, \dots, v\}$ . The claim that  $Q_j \subseteq \Sigma(S)$  now follows from the prehistoric lemma and the observation that

$$\Sigma(S) \cap Q_j \supseteq (k_1 \wedge S_1) + \dots + (k_v \wedge S_v) + \Sigma(S_0),$$

since

$$|(k_1 \wedge S_1) + \cdots + (k_v \wedge S_v)| \geq |k_{i_0} \wedge S_{i_0}| \geq \min(h-1, h-u)$$

(by (2)) and

$$|\Sigma(S_0)| \geq 2t \geq \max(2, 2u)$$

sum to more than  $h = |H| = |Q_j|$ .

The argument in the case that  $t = 0$  is similar, except on this occasion we use that  $j$  may be expressed as

$$\sum_{i=1}^v ik_i = j$$

where  $0 \leq k_i \leq h$  for all  $i$ , and either  $0 < k_i < h$  for two values of  $i \in \{1, \dots, v\}$  or  $k_{i_0} \in \{1, h-1\}$  for some  $i_0$ . In the latter case we observe immediately that

$$|\Sigma(S) \cap Q_j| \geq |(k_1 \wedge S_1) + \cdots + (k_v \wedge S_v)| \geq |k_{i_0} \wedge S_{i_0}| = |S_{i_0}| = h,$$

which implies that  $Q_j \subseteq \Sigma(S)$  as required. In the former case we simply use the prehistoric lemma applied to the two sets  $k_i \wedge S_i$  for which  $0 < k_i < h$  and Theorem 3.2, as above to obtain  $Q_j \subseteq \Sigma(S)$ .  $\square$

We may now read out the bound

$$|\Sigma(S)| \geq \frac{|S|(|S|+1)}{2} + 1,$$

completing the proof of Proposition 4.1. We prove that the quantity  $\Delta := |\Sigma(S)| - |S|(|S|+1)/2$  satisfies  $2\Delta \geq 2$ , as required. By combining Lemma 4.4 with Claim III we obtain that

$$\begin{aligned} 2\Delta &= 2|\Sigma(S)| - |S|(|S|+1) \\ &\geq (hv(v+1) - 2uv - 2)h + 8t - (hv + t - u)(hv + t - u + 1) \\ &= h^2v^2 + h^2v - 2uhv - 2h + 8t - h^2v^2 - (2t - 2u + 1)hv - (t - u)(t - u + 1) \\ &= h^2v - 2h + 8t - (2t + 1)hv - (t - u)(t - u + 1), \end{aligned}$$

where the final line is obtained simply by canceling terms. We first complete the proof in the case that  $h \geq 4$ . We shall deal with the special cases  $h \in \{1, 2, 3\}$  separately. Since  $h \geq 4$  we have that  $vh \geq 4$  and so  $8t - (2t + 1)vh$  is decreasing in  $t$ . Note also that, since  $t \geq u$ , the term  $-(t - u)(t - u + 1)$  is also decreasing in  $t$ . Thus, the final expression above is decreasing in  $t$ . Since  $t \leq h/4$  (by Claim I), and  $u \geq 0$ , we have that

$$\begin{aligned} 2\Delta &\geq h^2v - \frac{h^2v}{2} - hv - \frac{h^2}{16} - \frac{h}{4} \\ &\geq h^2v \left(1 - \frac{1}{2} - \frac{1}{4} - \frac{1}{16} - \frac{1}{16}\right) \\ &= \frac{h^2v}{8} \\ &\geq 2. \end{aligned}$$

For the special cases  $h \in \{1, 2, 3\}$  we have that  $t = 0$  by Claim I, and  $u = 0$  by Claim II. One may easily check the result by hand for the case that  $h \in \{1, 2, 3\}$  and  $v = 1$ . So let us assume that  $v \geq 2$ . Proceeding as in the proof of Lemma 4.4 and using the fact that  $|\Sigma(S) \cap Q_j| \geq 1$  for  $j \in \{0, \ell\}$  one obtains that  $|\Sigma(S)| \geq (\ell - 1)h + 2$ . Combining this with the fact that  $t = u = 0$  and Claim III, we obtain that

$$\begin{aligned} 2\Delta &\geq h^2v^2 + h^2v - 2h + 4 - h^2v^2 - hv \\ &= h^2v - 2h + 4 - hv \end{aligned} \quad = \begin{cases} 2 & \text{if } h = 1, \\ 2v & \text{if } h = 2, \\ 6v - 2 & \text{if } h = 3. \end{cases}$$

Since each of these values is at least 2 we obtain that  $|\Sigma(S)| \geq 1 + |S|(|S| + 1)/2$ , thus completing the proof of Proposition 4.1.

#### 4.2 The case that $\hat{S}$ has a Vosper-representation: A proof of Lemma 4.2

In this section, we prove Lemma 4.2. That is, we show that if  $B, S$  are subsets of a finite abelian group  $G$  with  $|B| = b \leq |G|/2$  and  $|S| = s \geq 3$ , and we have the additional properties that  $S$  generates  $G$ , that  $S \cap (-S) = \emptyset$  and that  $\hat{S}$  has a Vosper-representation, then

$$\max_{x \in S} \lambda_B(x) > s - \frac{s(s-3)}{b}.$$

This is sufficient since the second claim of Lemma 4.2 is an immediate consequence of the first.

Our proof proceeds via demonstrating a certain rate of expansion of the sets  $j\hat{S}$ , when  $S$  is as above. We say that a subset  $A$  of  $G$  is *faithful* if, for every integer  $j \geq 1$ , one has

$$|j\hat{A}| \geq \min(|G|, j(|\hat{A}| - 1) + 1).$$

It is clear that the required result follows immediately once we establish the following two lemmas.

**Lemma 4.5.** *Let  $G$  be a finite abelian group, and let  $S \subseteq G$ . Assume  $S$  generates  $G$  and that  $\hat{S}$  has a Vosper-representation. Then  $S$  is faithful.*

**Lemma 4.6.** *Let  $G$  be a finite abelian group, and let  $B, S$  be subsets of  $G$  with  $|B| = b \leq |G|/2$  and  $|S| = s \geq 3$ . Assume that  $S \cap (-S) = \emptyset$  and  $S$  is faithful. Then*

$$\max_{x \in S} \lambda_B(x) > s - \frac{s(s-3)}{b}.$$

We begin with some initial observations that we shall use in our proof of Lemma 4.5. Let  $G$  be a finite abelian group and  $S \subseteq G$  a generating subset with  $|S| = s \geq 3$  and such that  $\hat{S}$  has a Vosper-representation. Recall that  $\hat{S} = S \cup \{0\} \cup (-S)$  and let  $H$  be a subgroup of  $G$  such that

$$|\hat{S} + H| < \min(|G|, |\hat{S}| + |H|) \tag{10}$$

and with  $\phi(\hat{S})$  being a Vosper subset in  $G/H$ .

We first establish a basic lemma.

**Lemma 4.7.**  $2\hat{S}$  is  $H$ -periodic.

As we shall see, Lemma 4.7 is an elementary consequence of (10). We choose to write  $\hat{S}_Q$  for  $\hat{S} \cap Q$  for each coset  $Q$  of  $H$ . So that

$$\hat{S} = \bigcup_{Q \in \phi(\hat{S})} \hat{S}_Q.$$

The following two facts, together with the prehistoric lemma, are all that we require to deduce Lemma 4.7. Equation (10) is used in the proof of each of the facts.

**Fact 1.** If  $Q, R \in \phi(\hat{S})$  are two  $H$ -cosets with  $Q \neq R$ , then

$$\begin{aligned} |\hat{S}_Q| + |\hat{S}_R| &\geq 2|H| - |(\hat{S} + H) \setminus \hat{S}| \\ &> |H|. \end{aligned}$$

**Fact 2.** If  $Q \in \phi(\hat{S})$  is an  $H$ -coset with  $Q \neq H$ , then Fact 1 implies

$$\begin{aligned} |\hat{S}_Q| + |\hat{S}_Q| &= |\hat{S}_Q| + |\hat{S}_{-Q}| \\ &> |H|. \end{aligned}$$

*Proof of Lemma 4.7.* By Facts 1 and 2 we have that

$$|\hat{S}_Q| + |\hat{S}_R| > |H|$$

for all pairs  $Q, R \in \phi(\hat{S})$  other than  $(Q, R) = (H, H)$ . It follows by the prehistoric lemma that

$$\hat{S}_Q + \hat{S}_R = \hat{S}_Q + \hat{S}_R + H$$

for all pairs  $Q, R \in \phi(\hat{S})$  other than  $(Q, R) = (H, H)$ . Since  $H$  may be represented by  $Q + (-Q)$  for any  $Q \in \phi(\hat{S}) \setminus \{H\}$ , this establishes that  $2\hat{S} = 2\hat{S} + H$ , i.e.,  $2\hat{S}$  is  $H$ -periodic, as required.  $\square$

An immediate consequence of Lemma 4.7 is that  $j\hat{S}$  is  $H$ -periodic for all  $j \geq 2$ . It then follows that  $j\hat{S}$  consists precisely of all elements that belong to  $H$ -cosets  $Q \in j\phi(\hat{S})$ . In particular

$$|j\hat{S}| = |H||j\phi(\hat{S})| \quad \text{for all } j \geq 2. \quad (11)$$

Now, we prove that  $S$  is faithful.

*Proof of Lemma 4.5.* Let  $t \in \mathbb{N}$  be the greatest integer such that  $t\hat{S} \neq G$ . It is immediate that  $S$  is faithful in the case that  $t = 1$ . In the case that  $t \geq 2$  we shall in fact prove that

$$|j\hat{S}| \geq \begin{cases} j|\hat{S}| & \text{for } j = 1, \dots, t-1 \\ j|\hat{S}| - 1 & \text{for } j = t \\ |G| & \text{for } j > t \end{cases}$$



which clearly implies that  $S$  is faithful. The claimed bound is trivial for  $j > t$  (by the definition of  $t$ ). For  $j = 1, \dots, t-1$  we note that the required bounds follow directly from (11) and the bounds

$$|j\phi(\hat{S})| \geq j|\phi(\hat{S})| \quad j = 1, \dots, t-1,$$

which we now prove by induction on  $j$ . The base case  $j = 1$  is trivial. For  $j = 2, \dots, t-1$ , we obtain by the Vosper property of  $\phi(\hat{S})$  and the induction hypothesis that

$$|j\phi(\hat{S})| = |(j-1)\phi(\hat{S}) + \phi(\hat{S})| \geq \min(|G/H| - 1, j|\phi(\hat{S})|).$$

If the bound  $|j\phi(\hat{S})| \geq j|\phi(\hat{S})|$  is obtained then the proof of the induction step is complete, so we may assume for contradiction that  $|j\phi(\hat{S})| = |G/H| - 1$ . However, in this case  $|j\phi(\hat{S})| + |\phi(\hat{S})| > |G/H|$ , and so  $(j+1)\phi(\hat{S}) = G/H$  by the prehistoric lemma. It follows that  $(j+1)\hat{S} = G$ , a contradiction since  $j+1 \leq t$ . For the remaining case that  $j = t$  we use the Vosper property of  $\phi(\hat{S})$  and the result  $|(t-1)\phi(\hat{S})| \geq (t-1)|\phi(\hat{S})|$  obtained above to give that

$$|t\phi(\hat{S})| \geq |(t-1)\phi(\hat{S}) + \phi(\hat{S})| \geq \min(|G/H| - 1, t|\phi(\hat{S})|). \quad (12)$$

If  $t|\phi(\hat{S})| \leq |G/H| - 1$  then the minimum is attained at  $t|\phi(\hat{S})|$  and the claimed bound is proved. If  $t|\phi(\hat{S})| > |G/H|$  then  $|\phi(\hat{S})| + |(t-1)\phi(\hat{S})| > |G/H|$ , and so  $t\phi(\hat{S}) = G/H$  by the prehistoric lemma, and  $t\hat{S} = G$ , a contradiction. In the remaining case we have  $|G/H| - 1 < t|\phi(\hat{S})| \leq |G/H|$ , and so (12) gives us that  $|t\phi(\hat{S})| \geq t|\phi(\hat{S})| - 1$ . Combining this fact with the observation  $|H||\phi(\hat{S})| \geq |\hat{S}| + (|H| - 1)/2$  (which follows from Claim I of Section 4.1, for example) we obtain that

$$\begin{aligned} |t\hat{S}| &= |H||t\phi(\hat{S})| \\ &\geq |H|(t|\phi(\hat{S})| - 1) \\ &\geq t|\hat{S}| + t\left(\frac{|H| - 1}{2}\right) - |H| \\ &\geq t|\hat{S}| - 1. \end{aligned}$$

□

Having established that  $S$  is faithful we now prove that this is sufficient to guarantee the required bound on  $\max_{x \in S} \lambda_B(x)$ . The proof follows (more or less step by step) the proof of [9, Lemma 3.1].

*Proof of Lemma 4.6.* We write

$$\alpha = \max_{x \in S} \lambda_B(x),$$

and note that in fact  $\lambda_B(x) \leq \alpha$  for all  $x \in \hat{S}$ . Let  $t \leq |G| - 1$  be a positive integer and set

$$t = 2rs + q, \quad \text{where } 0 \leq q \leq 2s - 1.$$

Since  $S$  is faithful the bounds  $|j\hat{S} \setminus \{0\}| \geq \min(|G| - 1, 2js) \geq 2js$  for  $j = 1, \dots, r$ , and  $|(r+1)\hat{S} \setminus \{0\}| \geq \min(|G| - 1, 2(r+1)s) \geq t$  hold. Hence one may select a sequence of

disjoint sets  $C_j \subseteq G \setminus \{0\} : j = 1, \dots, r+1$  such that  $C_j \subseteq j\hat{S}$  for each  $j = 1, \dots, r+1$ , and with  $|C_j| = 2s : j = 1, \dots, r$ ,  $|C_{r+1}| = q$ . Set  $C = \bigcup_{j=1}^{r+1} C_j$ , and note that  $C \subseteq G \setminus \{0\}$  has cardinality  $t = 2rs + q$ . Our proof of the lemma proceeds via proving upper and lower bounds on the quantity  $\sum_{c \in C} \lambda_B(c)$ .

The lower bound on  $\sum_{c \in C} \lambda_B(c)$  is given immediately by Lemma 3.3:

$$\sum_{c \in C} \lambda_B(c) \geq |C||B| - |B|^2 + |B| = tb - b^2 + b.$$

For the upper bound on  $\sum_{c \in C} \lambda_B(x)$  we use the sub-additivity of  $\lambda_B(x)$  ensured by Lemma 3.3. Each element  $c \in C_j \subseteq j\hat{S}$  may be expressed as a sum

$$c = x_1 + \dots + x_j$$

where  $x_1, \dots, x_j$  are (not necessarily distinct) elements of  $\hat{S}$ , and so, by the sub-additivity of  $\lambda_B(x)$  (Lemma 3.3), we have  $\lambda_B(c) \leq \lambda_B(x_1) + \dots + \lambda_B(x_j) \leq j\alpha$ . It follows that

$$\sum_{c \in C_j} \lambda_B(c) \leq |C_j|j\alpha \quad j = 1, \dots, r+1,$$

and

$$\begin{aligned} \sum_{c \in C} \lambda_B(c) &\leq \sum_{j=1}^{r+1} |C_j|j\alpha \\ &= \alpha \sum_{j=1}^r 2js + \alpha q(r+1) \\ &= \alpha(r+1)(rs + q) \\ &= \frac{\alpha(t - q + 2s)(t + q)}{4s} \\ &\leq \frac{\alpha(t + s)^2}{4s}, \end{aligned}$$

where the final inequality follows since the penultimate expression is maximised when  $q = s$ .

Combining our bound on  $\sum_{c \in C} \lambda_B(c)$  yields the inequality

$$\alpha \geq \frac{4sb(t - b + 1)}{(t + s)^2}.$$

In particular, since  $2b - 3 \leq |G| - 1$ , we may set  $t = 2b - 3$ . It follows that

$$\begin{aligned} \alpha &\geq \frac{4sb(b - 2)}{(2b - 3 + s)^2} \\ &\geq s \left( \frac{b - 2}{b} \right) \left( 1 - \frac{s - 3}{b} \right) \\ &> s - \frac{s(s - 3)}{b}, \end{aligned}$$

where we have used  $s \geq 3$ . □

### 4.3 The stronger bound in the case that $|G|$ is odd: A proof of Lemma 4.3

Lemma 4.3 is effectively a strengthening of Lemma 4.2 established in the previous section, so it should not be surprising that the proof has many similarities to that given above. Proving stronger bounds on the cardinalities  $|j\hat{S}| : j \geq 2$  (in fact bounds identical to those proved by Olson in  $\mathbb{Z}_p$ ) is an essential improvement. The proof of Lemma 4.3 is completed by proving the following two lemmas. A subset  $A$  of  $G$  will be called *super faithful* if, for every integer  $j \geq 1$ , one has

$$|j\hat{A}| \geq \min(|G|, j(|\hat{A}| + 1) - 1).$$

**Lemma 4.8.** *Let  $G$  be a finite abelian group of odd order, and let  $S \subseteq G$ . Assume  $S$  generates  $G$  and that  $\hat{S}$  has a Vosper-representation. Then  $S$  is super faithful.*

**Lemma 4.9.** *Let  $G$  be a finite abelian group of odd order, and let  $B, S$  be subsets of  $G$  with  $|B| = b \leq |G|/2$  and  $|S| = s \geq 3$ . Assume that  $S \cap (-S) = \emptyset$  and  $S$  is super faithful. Let also  $t$  be an integer,  $1 \leq t \leq |G| - 1$ , and set*

$$t = r(2s + 2) + q, \text{ where } -1 \leq q \leq 2s.$$

*Then, there exists  $x \in S$  such that*

$$\lambda_B(x) \geq \frac{4(s+1)b(t-b+1)}{t(t+2s+6) + q(2s-q-2)}.$$

We proceed directly to the proof of the lemmas.

*Proof of Lemma 4.8.* Let  $G$  be a finite abelian group of odd order and let  $S \subseteq G$  be a generating subset with  $|S| = s \geq 3$  and such that  $\hat{S}$  has a Vosper-representation. Let  $H$  be a subgroup of  $G$  such that

$$|\hat{S} + H| < \min(|G|, |\hat{S}| + |H|) \tag{13}$$

and with  $\phi(\hat{S})$  being a Vosper subset in  $G/H$ . Let  $t \in \mathbb{N}$  be the greatest integer such that  $t\hat{S} \neq G$ . It is immediate that  $S$  is super faithful in the case that  $t = 1$ . Thus we may assume that  $t \geq 2$ . Using the fact, established in Section 4.2, that  $j\hat{S}$  is  $H$ -periodic for all  $j \geq 2$  it suffices to prove that

$$|j\phi(\hat{S})| \geq j(|\phi(\hat{S})| + 1) - 1 \tag{14}$$

for  $j = 2, \dots, t$ , as this implies

$$|j\hat{S}| = |H||j\phi(\hat{S})| \geq j|\phi(\hat{S})||H| + (j-1)|H| \geq j|\hat{S}| + (j-1).$$

We prove that (14) holds by induction on  $j$ , using the Vosper property of  $\phi(\hat{S})$  and a parity trick of Olson. Note that (14) trivially holds for  $j = 1$ . For  $j = 2, \dots, t$ , we obtain by the Vosper property of  $\phi(\hat{S})$  that

$$|j\phi(\hat{S})| \geq \min(|G/H| - 1, |(j-1)\phi(\hat{S})| + |\phi(\hat{S})|).$$

Since  $|G|$  is odd, so is  $|G/H|$ . In addition, the fact that  $j\phi(\hat{S})$  is symmetric and contains 0 implies that  $|j\phi(\hat{S})|$  is odd. Thus,  $|j\phi(\hat{S})| \geq |G/H| - 1$  cannot occur, otherwise we would have  $|j\phi(\hat{S})| \geq |G/H|$ , so that  $j\phi(\hat{S}) = G/H$ , which implies  $j\hat{S} = G$ , a contradiction.

Therefore,

$$|j\phi(\hat{S})| \geq |(j-1)\phi(\hat{S})| + |\phi(\hat{S})|.$$

Then, the induction hypothesis, and the very same argument of parity again ( $|j\phi(\hat{S})|$  is odd), yields

$$\begin{aligned} |j\phi(\hat{S})| &\geq |(j-1)\phi(\hat{S})| + |\phi(\hat{S})| + 1 \\ &\geq (j-1) \left( |\phi(\hat{S})| + 1 \right) - 1 + |\phi(\hat{S})| + 1 \\ &= j \left( |\phi(\hat{S})| + 1 \right) - 1, \end{aligned}$$

as required.  $\square$

*Proof of Lemma 4.9.* We write

$$\alpha = \max_{x \in \hat{S}} \lambda_B(x),$$

and note that in fact  $\lambda_B(x) \leq \alpha$  for all  $x \in \hat{S}$ . Now, let  $t$  be as in the statement of the lemma. One can distinguish the following two cases.

- If  $t \leq 2s$ , then  $r = 0$  and  $q = t$ , let  $C$  consist of  $t$  elements in  $\hat{S} \setminus \{0\}$ . Thus, we obtain

$$\sum_{c \in C} \lambda_B(c) \leq \alpha t = \alpha \left( \frac{t(t+2s+6) + q(2s-q-2)}{4(s+1)} \right).$$

- If  $t \geq 2s+1$ , then  $r \geq 1$ . Since  $S$  is super faithful the bounds  $|j\hat{S} \setminus \{0\}| \geq \min(|G| - 1, j(2s+2) - 2) \geq j(2s+2) - 2$  for  $j = 1, \dots, r$ , and  $|(r+1)\hat{S} \setminus \{0\}| \geq \min(|G| - 1, (r+1)(2s+2) - 2) \geq t$  hold. Hence one may select a sequence of disjoint sets  $C_j \subseteq G \setminus \{0\} : j = 1, \dots, r+1$  such that  $C_j \subseteq j\hat{S}$  for each  $j = 1, \dots, r+1$ , and with  $|C_j| = 2s : j = 1, |C_j| = 2s+2 : j = 2, \dots, r, |C_{r+1}| = q+2$ . Set  $C = \bigcup_{j=1}^{r+1} C_j$ , and note that  $C \subseteq G \setminus \{0\}$  has cardinality  $t = r(2s+2) + q$ . Our proof of the lemma proceeds via proving upper and lower bounds on the quantity  $\sum_{c \in C} \lambda_B(c)$ .

The lower bound on  $\sum_{c \in C} \lambda_B(c)$  is given immediately by Lemma 3.3:

$$\sum_{c \in C} \lambda_B(c) \geq |C||B| - |B|^2 + |B| = tb - b^2 + b.$$

For the upper bound on  $\sum_{c \in C} \lambda_B(c)$  we use the sub-additivity of  $\lambda_B(x)$  (as in the proof of Lemma 4.6) which gives us that  $\lambda_B(c) \leq j\alpha$  for all  $c \in C_j$ . It follows that

$$\begin{aligned} \sum_{c \in C} \lambda_B(c) &\leq 2s\alpha + 2(2s+2)\alpha + \dots + r(2s+2)\alpha + (q+2)(r+1)\alpha \\ &= \frac{\alpha}{2} (r(r+1)(2s+2) + 2(q+2)(r+1) - 4) \\ &= \frac{\alpha}{2} ((r+1)(t+q+4) - 4) \\ &= \alpha \left( \frac{t(t+2s+6) + q(2s-q-2)}{4(s+1)} \right). \end{aligned}$$

Combining our bound on  $\sum_{c \in C} \lambda_B(c)$  yields the inequality

$$\alpha \geq \frac{4(s+1)b(t-b+1)}{t(t+2s+6)+q(2s-q-2)},$$

as required. □

## References

- [1] E. BALANDRAUD *An addition theorem and maximal zero-sum free sets in  $\mathbb{Z}/p\mathbb{Z}$* , Israel J. Math., to appear.
- [2] M. DEVOS, L. GODDYN, B. MOHAR AND R. ŠÁMAL *A quadratic lower bound for subset sums*, Acta Arith. **129** (2007), 187-195.
- [3] J. A. DIAS DA SILVA AND Y. OULD HAMIDOUNE *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. **26** (1994), 140-146.
- [4] P. ERDŐS AND H. HEILBRONN *On the addition of residue classes mod  $p$* , Acta Arith. **9** (1964), 149-159.
- [5] M. FREEZE, W. GAO AND A. GEROLDINGER *The critical number of finite abelian groups*, J. Number Theory **129** (2009), 2766-2777.
- [6] B. GIRARD, S. GRIFFITHS AND Y. OULD HAMIDOUNE  *$k$ -sums in abelian groups*, submitted.
- [7] S. GRIFFITHS *Asymptotically tight bounds on subset sums*, Acta Arith. **138** (2009), 53-72.
- [8] Y. OULD HAMIDOUNE *Adding distinct congruence classes*, Combin. Probab. Comput. **7** (1998), 81-87.
- [9] Y. OULD HAMIDOUNE, A. S. LLADÓ AND O. SERRA *On complete subsets of the cyclic group*, J. Comb. Theory, Ser. A **115** (2008), 1279-1285.
- [10] Y. OULD HAMIDOUNE AND A. PLAGNE *A new critical pair theorem applied to sum-free sets in abelian groups*, Comment. Math. Helv. **79**(1) (2004), 183-207.
- [11] M. KNESER *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459-484.
- [12] M. KNESER *Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429-434.
- [13] M. B. NATHANSON *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. **165**, Springer, 1996.
- [14] J. E. OLSON *An addition theorem modulo  $p$* , J. Comb. Theory **5** (1968), 45-52.

- [15] J. E. OLSON *Sums of sets of group elements*, Acta Arith. **28** (1975), 147-156.
- [16] T. TAO AND V. H. VU *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics **105** (2006), Cambridge Press University.